Secure quantum key distribution network with Bell states and local unitary operations *

Chun-Yan Li[1,2,3], Hong-Yu Zhou[1,2,3], Yan Wang[1,2,3], Fu-Guo Deng[1,2,3†]
[1] *The Key Laboratory of Beam Technology and Material Modification of Ministry of Education, Beijing Normal University, Beijing 100875, China*
[2] *Institute of Low Energy Nuclear Physics, and Department of Material Science and Engineering, Beijing Normal University, Beijing 100875, China*
[3] *Beijing Radiation Center, Beijing 100875, China*
(Dated: February 5, 2008)

We propose a theoretical scheme for secure quantum key distribution network following the ideas in quantum dense coding. In this scheme, the server of the network provides the service for preparing and measuring the Bell states, and the users encodes the states with local unitary operations. For preventing the server from eavesdropping, we design a decoy when the particle is transmitted between the users. It has high capacity as one particle carries two bits of information and its efficiency for qubits approaches 100%. Moreover, it is not necessary for the users to store the quantum states, which makes this scheme more convenient for application than others.

PACS numbers: 3.67.Dd, 03.67.Hk, 03.65.Ud

Quantum key distribution (QKD), the most advanced application of the principles in quantum mechanics within the field of information, such as the uncertainty principle and quantum correlations, provides a secure way for two remote parties, say Alice and Bob to create a randomly binary string that can be used as a private key with which they can communicate securely using Vernam one-time pad crypto-system [1]. In the key transmission with classical line only, a vicious eavesdropper, Eve can monitor the line freely without leaving a trace. But the uncertainty principle assures that Eve cannot copy an unknown quantum state of single particle [2]. In 1984, Bennett and Brassard [3] designed the first theoretical model for quantum key distribution based on noncloning theorem [2], called BB84 QKD protocol. Quantum correlations of entangled particles or wave-packets also help people to do key distribution in an unconditionally secure way. Ekert [4] proposed another QKD scheme based on the correlation of Einstein-Podolsky-Rosen (EPR) pair, the maximal entangled state of two particles in 1991. To date, a great number of works have been done on QKD both in theoretical aspects [5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15] and in experimental implementations [16, 17].

Most of the existing QKD protocols concentrate on point-to-point key distribution between two remote parties. The practical application of QKD requires the communication of any-to-any key distribution on a network, same as the classical communication network (world web). Unfortunately, there are only a little of works focused on multi-user quantum key distribution (MUQKD) [18, 19, 20, 21, 22] on a passive optical network. Some [18, 19, 20] of them choose single photons as quantum information carrier (QIC) and measure them with two sets of measuring bases (MBs), the rectilinear basis σ_z and the diagonal basis σ_x. Their total efficiency η_t is low. η_t is defined as [8, 9]

$$\eta_t = \frac{b_s}{q_t + b_t}, \tag{1}$$

where b_s is the number of bits in the key, q_t is the number of qubits used, and b_t is the number of classical bits exchanged between the parties. For example, the efficiency η_t in Ref. [19] is lower than $\frac{1}{16}$ as no more than $\frac{1}{8}$ QIC can be used as the qubits in the raw key. Xue et. al. proposed a MUQKD protocol with the combination of two-particle product states and entangled states following the ideas in Ref. [7], and almost all of the instances can be used as the raw key and two particles can carry one bit of quantum information. In the MUQKD scheme [22], EPR pairs are used as QIC and are transmitted with two quantum channels. The four local unitary operations represent four kinds of coding. It is the generalization of the Long-Liu point-to-point QKD protocol [9] into the case with many users on a passive optical network. With quantum storage (quantum memory) [23, 24, 25, 26], its efficiency for qubit $\eta_q \equiv \frac{q_u}{q_t}$ approaches 100% and its total efficiency η_t approaches 50% as all the EPR pairs are useful for the raw key and only two bits of classical information are exchanged for two qubits, where q_u is the useful qubits. Certainly, the technique of quantum storage is not fully developed at present. However it is a vital ingredient for quantum computation and quantum information, and there has been great interests in developing it [23, 24, 25, 26]. It is believed that this technique will be available in the future. With quantum memory, many new applications can be constructed, such as quantum computation [27], quantum secure direct communication [28, 29, 30, 31, 32, 33, 34, 35, 36, 37] and quantum secret splitting [38, 39].

In this paper, we want to introduce a MUQKD scheme

*published in *Chinese Physics Letters* **22** (5), 1049-1052 (2005).
†E-mail: fgdeng@bnu.edu.cn

with EPR pairs following the ideas in quantum dense coding [40]. In this scheme, the users on the network need only perform single-particle measurement and exploit a decoy technique, replacing some of the particles in the original QIC with those whose states are unknown for others, to guarantee its security. The information is encoded on the states with four local unitary operations. The efficiency and the capacity of this MUQKD scheme are maximal, same as those in Ref. [22]. Moreover it does not require the users to store the quantum states received and only one particle in each EPR pair runs through the quantum channel, which make this MUQKD scheme more convenient for the practical application.

An EPR pair is in one of the four Bell states shown as follows[9, 11, 22]:

$$\left|\psi^{-}\right\rangle_{AB}=\frac{1}{\sqrt{2}}(\left|0\right\rangle_{A}\left|1\right\rangle_{B}-\left|1\right\rangle_{A}\left|0\right\rangle_{B}), \tag{2}$$

$$\left|\psi^{+}\right\rangle_{AB}=\frac{1}{\sqrt{2}}(\left|0\right\rangle_{A}\left|1\right\rangle_{B}+\left|1\right\rangle_{A}\left|0\right\rangle_{B}), \tag{3}$$

$$\left|\phi^{-}\right\rangle_{AB}=\frac{1}{\sqrt{2}}(\left|0\right\rangle_{A}\left|0\right\rangle_{B}-\left|1\right\rangle_{A}\left|1\right\rangle_{B}), \tag{4}$$

$$\left|\phi^{+}\right\rangle_{AB}=\frac{1}{\sqrt{2}}(\left|0\right\rangle_{A}\left|0\right\rangle_{B}+\left|1\right\rangle_{A}\left|1\right\rangle_{B}). \tag{5}$$

The four local unitary operations U_i $(i=0,1,2,3)$ can transform one of the Bell states into each other.

$$\begin{aligned} U_0&=\left|0\right\rangle\left\langle 0\right|+\left|1\right\rangle\left\langle 1\right|, \quad U_1=\left|0\right\rangle\left\langle 1\right|-\left|1\right\rangle\left\langle 0\right|, \\ U_2&=\left|1\right\rangle\left\langle 0\right|+\left|0\right\rangle\left\langle 1\right|, \quad U_3=\left|0\right\rangle\left\langle 0\right|-\left|1\right\rangle\left\langle 1\right|. \end{aligned} \tag{6}$$

For example,

$$I\otimes U_0|\phi^{+}\rangle = |\phi^{+}\rangle, \quad I\otimes U_1|\phi^{+}\rangle=-|\psi^{-}\rangle, \tag{7}$$

$$I\otimes U_2|\phi^{+}\rangle = |\psi^{+}\rangle, \quad I\otimes U_3|\phi^{+}\rangle=|\phi^{-}\rangle, \tag{8}$$

where $I=U_0$ is the 2×2 identity matrix.

First, let us compare the quantum dense coding with the Long-Liu point-to-point QKD scheme. In quantum dense coding [40], the QIC is the EPR pairs transmitted in one by one and one of the two particles in each pair runs forth and back from the receiver of information, Carol to the sender Bob. The other particle is hold in the hand of Carol. The information is encoded on the state with the four unitary operations U_i chosen randomly by Bob. After the particle encoded returns to Carol, she performs the Bell state measurement on the EPR pair and reads out the information about the operation. In this way, a particle can carry two bits of information with running forth and back. In the Long-Liu point-to-point QKD protocol [9], the EPR pairs are transmitted by using two split channels in a quantum data block, which is necessary for QSDC [28, 29, 30] but not for QKD as the analysis of the security in QKD is just a post-processing. The advantage of Long-Liu QKD protocol [9] is that the loss of the qubits is lower by far than that in quantum dense coding when there are noise and loss in the quantum channel as all the QIC are transmitted from the sender to the receiver once. This advantage will disappear in the case [22] with many user on a network.

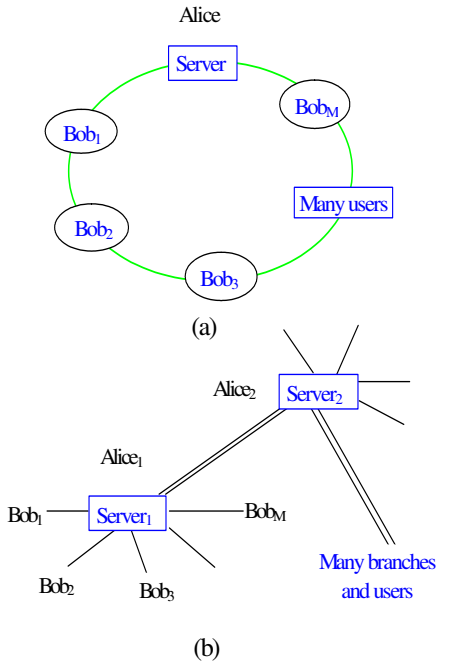

FIG. 1: The topological structure of the network, similar to those in Refs. [18, 19, 20, 21, 22]: (a) loop-configuration network; (b) star-configuration network.

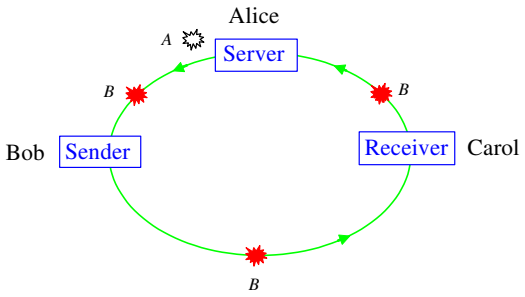

FIG. 2: The subsystem of the network in this MUQKD scheme. The server provides the service for preparing and measuring the Bell states, Bob and Carol choose randomly the control mode and the coding mode for the particles received. They sends the particles to next one when they choose the coding mode, otherwise they perform single-particle measurement on the particles received with one of the two MBs randomly. For preventing the server from eavesdropping, Bob exploit the decoy technique with a certain probability, i.e., replacing the original particle with his one prepared with one of the two MBs.

Now we discuss our MUQKD scheme in detail. Although the topological structure of the network can be loop or star, similar to those in Refs. [18, 19, 20, 21, 22] shown in Fig.1, its subsystem can be simplified to that in Fig.2, composed of the server (Alice), the sender (Bob)

and the receiver (Carol). Suppose Alice is the server of the sender, Bob. If Carol is in another branch of the network, her server, say $Alice_i$ provides the quantum channel for her to communicate with Bob only in a given time slot [21, 22]. So this MUQKD scheme is explicit if we describe clearly the subsystem in Fig.2. For the integrality of this MUQKD scheme, we describe the steps in detail, including some same as those in Ref. [22].

(S1) All the users on the network agree that the four unitary operations, U_0, U_1, U_2 and U_3 represent the bits 00, 01, 10 and 11, respectively. The server Alice prepares the QIC in the original state $|\phi^+\rangle_{AB}$.

(S2) Alice sends the particle B to Bob and keeps the particle A in home.

(S3) Bob chooses randomly the control mode or the coding mode, similar to that in Ref. [41]. When he chooses the control mode, he performs the single-particle measurement on particle B by choosing the two MBs, σ_z or σ_x with the same probability. He tell Alice his MB for the particle B and requires her measure the particle A with the same MB. Alice publishes the result of the measurement, which is a sample for eavesdropping check during the phase that the particle is transmitted between Alice and Bob.

If Bob chooses the coding mode, he chooses randomly one of the four unitary operations $\{U_i\}$, say U_B and performs it on the particle B, and then sends the particle to Carol.

Surely, in order to prevent Alice (the server who prepares the QIC) from eavesdropping the quantum channel between Bob and Carol, Bob should choose the third mode, the decoy mode for the particle B with a certain probability. In this time, he replaces the particle B with the particle d in state $|\chi\rangle_d \in \{|0\rangle, |1\rangle, |+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ prepared by himself with two MBs σ_z and σ_x randomly in advance, and then sends it to Carol. Bob measures the particle B with the same MB as that for preparing the particle d.

(S4) Carol performs her operation on particle B similar to Bob except for the third mode. When she chooses the control mode, she measures the particle with two MBs randomly and requires Alice do the correlated measurement with the same MB on the particle A and publish the result; otherwise she operates the particle with one of the four unitary operations randomly, say U_C and then sends it to Alice.

(S5) Alice takes a joint Bell state measurement on the EPR pair after she receives the particle returned from Carol. She announces in public the result of the measurement, $U_A = U_B \otimes U_C$ which is the combined operations performed by Bob and Carol.

(S6) Carol obtains the bits encoded on the particle B done by Bob according to her operations U_C and the information published by Alice, $R_C = U_A \otimes U_C$.

(S7) Alice, Bob and Carol repeat the processes above for distributing the bits until they can obtain enough results R_c. Bob tells Carol the position where she replaces the particle B with her particle d.

(S8) Alice, Bob and Carol choose some of the instances as samples for eavesdropping check and complete the analysis of the error rates of the samples.

In detail, there are several sequences of the samples for eavesdropping check. One is the results that Bob obtains with the control mode, say $s_{_{Bc}}$. One is the results obtained by Carol with the control mode, say $s_{_{Cc}}$ which are divided into two parts, $s_{_{Cc0}}$ and $s_{_{Cc1}}$ come from the measurements on the particle B and the particle d respectively. The third is the results chosen by Bob randomly from the instances for which both Bob and Carol choose coding mode, say $s_{_w}$. Alice, Bob and Carol exploit the refined error analysis technique [7] for checking eavesdropping.

(S9) If all the error rates are lower than the threshold, Bob and Carol can distill the key with error correction and privacy amplification [27] from the results R_{BC} for which they both choose the code mode. Otherwise, they abandon the results and repeat the quantum communication from the beginning.

Now, let us discuss some issues about the security of this MUQKD scheme.

There are two classes of eavesdroppers in this MUQKD scheme. One is the vicious eavesdropper, Eve who does not have the access to the particle A in each EPR pair. The other is the server, Alice who provides the QIC for the communication and keeps the particle A in the whole process of the quantum communication. For the former, the quantum communication between two parties in the subsystem of this MUQKD scheme equals to Bennett-Brassard-Mermin (BBM) QKD protocol [5] with or without the help of the third parties, i.e., publishing his/her unitary operations or results. For example, with the help of Bob's, Alice and Carol can complete the analysis of the security of the quantum communication in the phase that the QIC runs from Bob to Carol. The security is embodied to the fact that the action of Eve's will disturb the quantum systems and will be detected by Alice and Carol by analyzing the error rate of the results $s_{_{Cc0}}$ obtained by Carol with the control mode. From the view of eavesdropping check for Eve, this MUQKD scheme is equal to the BBM QKD protocol [5], similar to that in the QSDC protocol [28]. The BBM QKD protocol is proven unconditionally secure both in ideal condition [42] and in the case with noise [43]. So this MUQKD scheme is secure for Eve.

As Alice has the access to the particle A in each EPR pair, she can obtain the unitary operations U_B easily and will not be detected if Bob only chooses the control mode for eavesdropping check. That is, she performs Bell state measurement on the EPR pair after the coding done by Bob and then gets the information without leaving a trace. *With the decoy technique*, the story will be changed. Alice will be found out if she monitors the quantum channel between Bob and Carol as her actions will introduce errors in the samples $s_{_{Cc1}}$. For $s_{_{Cc1}}$ which are obtained from the particles d, half of the results can be used as the samples for eavesdropping check as the

probability that Bob and Charlie choose the same MB and then they can get the same results in principle is 50%. If there is an eavesdropper in the line, he/she will introduce the errors in the results as he/she does not know the MBs about the particles d and his/her action will disturb the quantum systems, similar to that in BB84 QKD protocol [3, 27]. The error rate introduced by an eavesdropper is 25% if he or she monitors all the quantum signal. The probability for choosing the decoy mode is similar to the case with the biased bases discussed in Refs. [7, 21].

There are some common features between this MUQKD scheme and that in Ref. [22]: (1) The QIC is EPR pair and the four local unitary operations represent the different information encoded on the states; (2) The efficiency for qubits η_q approaches 100% as almost all of the instance can be used as the useful qubits and the total efficiency η_t is 50%; (3) Both of them have high capacity; (4) The operations U_C performed by the receiver Carol are absolutely necessary for the QKD as they make others know nothing about the operations U_B with the results of the combined operations published by the server Alice $U_A = U_B \otimes U_C$ and cannot obtain the keys [22]; (5) The users need not prepare and measure the EPR pairs, and the server provides the services; (6) The users should have the ability for measuring a single particle with two MBs.

Of course, there are some differences in these two MUQKD schemes. Firstly, in this scheme there is only one of the two particles in each EPR pair running through the quantum channel, not both. Secondly, it is unnecessary for the users to store the QIC in this scheme, but necessary in [22]. For preventing Alice from eavesdropping the keys, Bob should exploit the decoy mode with a certain probability. As the decoy mode is only used for eavesdropping, the particle d can be a faint laser pulse if the QIC is photons in this scheme and any eavesdropping will be detected [14]. In this way, there is not difficulty for Bob to prepare the particle d, and this scheme is easier to be implemented than that in Ref. [22].

In summary, we have introduced a new multi-user quantum key distribution scheme following the ideas in quantum dense coding. This scheme is secure if the sender of the information chooses the decoy mode with a certain probability. It has high capacity and its efficiency for qubit approaches 100% as almost all the EPR pairs can used to transmit the information. There is only one of the two particles in each EPR pair running through the quantum channel, and then the loss of qubits is reduced when there is loss in the channel. Moreover, it does not require the users on the network store the quantum states and is more convenient for application than that in [22].

This work was supported by the National Natural Science Foundation of China under Grant Nos.10447106, 10435020, 10254002 and A0325401.

[1] Vernam G S 1926 *J. Amer. Inst. Elec. Eng.* **45** 109
[2] Wootters W K and Zurek W H 1982 *Nature* **299** 802
[3] Bennett C H and Brassad G 1984 *Proc. IEEE Int.Conf. on Computers, Systems and Signal Processing (Bangalore, India* (New York: IEEE) PP 175-179
[4] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[5] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[6] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[7] Lo H K, Chau H F and Ardehali M 2000 *Preprint* arXiv: quant-ph/0011056
[8] Cabello A 2000 *Phys. Rev. Lett.* **85** 5635
[9] Long G L and Liu X S 2002 *Phys. Rev.* A **65** 032302
[10] Zhang Y S, Li C F and Guo G C 2001 *Phys. Rev.* A **64** 024302
[11] Deng F G and Long G L 2003 *Phys. Rev.* A **68** 042315
[12] Gui Y Z, Han Z F, Mo X F and Guo G C 2003 *Chin. Phys. Lett.* **20** 608
[13] Han C, Xue P and Guo G C 2003 *Chin. Phys. Lett.* **20** 183
[14] Deng F G and Long G L 2004 *Phys. Rev.* A **70** 012311
[15] Deng F G, Long G L, Wang Y and Xiao L 2004 *Chin. Phys. Lett.* **21** 2097
[16] Kurtsiefer C, Zarda P, Halder M et. al. 2002 *Nature* **419** 450
[17] Gobby C, Yuan Z L and Shields A J 2004 *Appl. Phys. Lett.* **84** 3762
[18] Phoenix S J D, Barnett S M, Townsend P D and Blow K J 1995 *J. Mod. Opt.* **42** 1155
[19] Biham E, Huttner B and Mor T 1996 *Phys. Rev.* A **54** 2651
[20] Townsend P D 1997 *Nature* **385** 47
[21] Xue P, Li C F and Guo G C 2002 *Phys. Rev.* A **65** 022317
[22] Deng F G, Liu X S, Ma Y J, Xiao L and Long G L 2002 *Chin. Phys. Lett.* **19** 893
[23] Liu C, Dutton Z, Behroozi C H and Hau L V 2001 *Nature* **409** 490
[24] Philips D F, Fleischhauer A, Mair A et.al. 2001 *Phys. Rev. Lett.* **86** 783
[25] Sun C P, Li Y and Liu X F 2003 *Phys. Rev. Lett.* **91** 147903
[26] Wang K G and Zhu S Y 2002 *Chin. Phys. Lett.* **19** 60
[27] Nielsen M A and Chuang I L 2000 *Quantum computation and quantum information* (Cambridge University Press, Cambridge, UK)
[28] Deng F G, Long G L and Liu X S, 2003 *Phys. Rev.* A **68** 042317
[29] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319
[30] Yan F L and Zhang X Q 2004 *Eur. Phys. J.* B **41** 75
[31] Gao T, Yan F L and Wang Z X 2004 *Nuovo Cimento Della Societa Italiana Di Fisica* B **119** 313
[32] Gao T 2004 *Zeitschrift Fur Natureforshung Section* A **59** 597
[33] Cai QY and Li BW 2004 *Chin. Phys. Lett.* **21** 601
[34] Zhang Z J, Man Z X and Li Y 2004 *Phys. Lett.* A **333** 46
[35] L*ü* H, Yan X D, Zhang X Z 2004 *Chin. Phys. Lett.* **21** 2340

[36] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 18; 2005 *Chin. Phys. Lett.* **22** 22
[37] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev.* A **71** 044305
[38] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[39] Li Y M, Zhang K S and Peng K C 2004 *Phys. Lett.* A **324** 420
[40] Bennett C H. and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
[41] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[42] Inamori H, Rallan L and Vedral V 2001 *J. Phys.* A **34** 6913
[43] Waks E, Zeevi A and Yanamoto Y 2002 *Phys. Rev.* A **65** 052310